MAIL STOP APPEAL
BRIEF - PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicant:	H. Koike et al.	Attorney Docket No.:	**NAII116493 (new)** LEXW116493 (old)
Application No.:	09/710,203	Group Art Unit:	2131
Filed:	November 9, 2000	Examiner:	K. Abrishamkar
Title:	LOG FILE PROTECTION SYSTEM		

TRANSMITTAL OF REPLY BRIEF

Seattle, Washington 98101
November 14, 2006

TO THE COMMISSIONER FOR PATENTS:

Enclosed herewith for filing in the above-identified patent application is a Reply Brief. The Commissioner is hereby authorized to charge any fees under 37 C.F.R. §§ 1.16, 1.17 and 1.18 which may be required during the entire pendency of the application, or credit any overpayment, to Deposit Account No. 03-1740. This authorization also hereby includes a request for any extensions of time of the appropriate length required upon the filing of any reply during the entire prosecution of this application.

Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS[PLLC]

Reg. no. 46,649
for

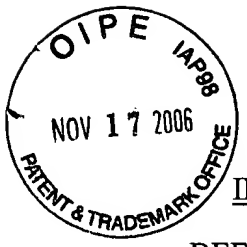
Shoko I. Leek
Registration No. 43,746
Direct Dial No. 206.695.1780

I hereby certify that this correspondence is being deposited with the U.S. Postal Service in a sealed envelope as first-class mail with postage thereon fully prepaid and addressed to Mail Stop Appeal Brief—Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the below date.

Date: November 14, 2006

SIL:vas

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS[PLLC]
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100



MAIL STOP APPEAL
BRIEF - PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicants:	H. Koike et al.	Attorney Docket No.:	**NAII116493 (new)** LEXW116493 (old)
Application No:	09/710,203	Art Unit: 2131 / Confirmation No.: 4596	
Filed:	November 9, 2000	Examiner: K. Abrishamkar	
Title:	LOG FILE PROTECTION SYSTEM		

APPELLANT'S REPLY BRIEF

Seattle, Washington

November 14, 2006

TO THE COMMISSIONER FOR PATENTS:

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

ARGUMENT

Responsive to the Examiner's Answer mailed September 15, 2006, appellant submits the following.

Appellant continues to believe that the rejection of all pending claims under 35 U.S.C. § 102(a), as identically disclosed in Schneier et al., was erroneous.

Schneier et al. fails to teach or suggest the claimed features directed to "periodically monitoring the plurality of identical log files for alteration or deletion" and "replacing the altered or deleted log file with an unaltered log file from the plurality of identical log files." Accordingly, Claims 1 and 26 of the present application, explicitly reciting these features, are not anticipated by Schneier et al.

In his Answer, the Examiner argued that Schneier et al. teaches "periodically monitoring the plurality of identical log files for alteration or deletion." Specifically, the Examiner stated that:

> Schneier states that "we only need U to communicate the log entries to T infrequently, at some period related to the frequency [with] which you expect [that] T may be compr[om]ised" (See Section 1, paragraph 11). This periodic communication between U (the untrusted machine creating the log files) and T (the trusted machine) is for the purpose of checking to see if the log files have been changed or destroyed . . . [T]he communication between the untrusted machine and the one or more servers is periodic, multiple identical log files are created and stored, and the periodic interaction between the untrusted machine and the one or more servers determines if a log file is changed or deleted. Therefore, the Examiner contends that Schneier does teach, "periodically monitoring the plurality of identical log files for alteration or deletion."
>
> (Examiner's Answer, page 5, last line - page 6, first paragraph. Emphasis added.)

The Examiner's main contention is that, in Schneier et al., because an untrusted machine U and one or more trusted machines (or servers) T are periodically communicating with each other, the purpose of the communication must somehow be to monitor log files to detect if they

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

have been changed or deleted. Note that the underlined portions of the Examiner's statement quoted above are his own words; they are not at all from Schneier et al. itself. Schneier et al., contrary to the Examiner's creative reading based on hindsight, does not teach or suggest "periodically monitoring the plurality of identical log files for alteration or deletion." Rather, Schneier et al. merely teaches periodically transferring a log file from an untrusted computer to a trusted computer, as more fully discussed below.

As appellant previously explained, the fundamental difference between the present invention and the technique described in Schneier et al. is that Schneier et al. is directed to securing a log file in an "untrusted computer U," such as an electronic wallet, which can be connected to a "trusted computer T," such as a server computer located at a bank. (Section 1, paragraph 5.) The technique achieves securing log files by adjusting the frequency at which the untrusted computer U transmits its log file to the trusted computer T, where the log file can be protected from intrusion. (Section 1, paragraph 11.) Nowhere in Schneier et al. is it disclosed or suggested that the log file that has been transmitted from the untrusted computer U to the trusted computer T is thereafter periodically monitored for alteration or deletion. Rather, what occurs periodically in Schneier et al. is the *transfer* of a log file from the untrusted computer U to the trusted computer T — not any monitoring of the log file for alteration or deletion.

Section 4.2 of Schneier et al. is titled "Replacing T with a Network of Insecure Peers," meaning that the "trusted computer T" can be replaced with a number of "untrusted computers U" in some cases. (Section 4.2, paragraphs 1-2.) Schneier et al. notes, though, that even if a number of "untrusted computers U" are provided to replace the trusted computer T, if an attacker compromises all of the untrusted computers U, then the integrity of a log file in any of these untrusted computers U can be compromised. (Section 4.2, paragraph 8.) As a solution to this problem, Schneier et al. proposes that an untrusted computer "U_0 should log the same data in

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

several parallel log files, with each log file using a different untrusted server as its trusted server." Thus, in this proposal also, the integrity of each of the "several parallel log files" is maintained based on its transmission to its "trusted server," and *not* based on the subsequent monitoring of all of the several parallel log files for alteration or deletion. Note that in Schneier et al., several parallel log files are simply transmitted to their respective "trusted" computers for protection, and are *not* monitored for alteration or deletion.

In the Examiner's Answer, the Examiner also contended that Schneier et al. teaches "replacing the altered or deleted log file with an unaltered log file from the plurality of identical log files." Specifically, the Examiner noted that:

> Schneier teaches storing a plurality of identical log files (Section 4.2). Furthermore, Schneier teaches that A_0, a log file, can be stored on n untrusted machines, and if A_0 is deleted, that A_0 can be recovered from any m of the machines (Section 4.2, page 8, column 2). Furthermore, Schneier states that if a log file has been compromised, that the user can "restore it from a clean backup" (Section 5, paragraph 1).
>
> (Examiner's Answer, page 7, first paragraph. Emphasis added.)

Appellant respectfully notes that A_0, which the Examiner equates as the "log file" of the present invention, is actually "a random starting point" formed in an untrusted machine for the purpose of establishing a secure connection with another untrusted machine. (Section 4.2, page 8, column 1). In fact, for the purpose of security, the untrusted machine that initially forms A_0 does not even "store A_0 in the clear, as this could lead to replay attacks." (Section 3.2, page 5, column 1). Therefore, the Examiner's reading of the "random starting point" A_0 as something equivalent to the log file is erroneous.

Appellant further submits that the Examiner's reliance on Section 5 for the teaching of "restor[ing a compromised log file] from a clean backup" is erroneous. As appellant has previously explained, Section 5, paragraph 1 of Schneier et al. in fact describes a conventional

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

file backup/restore system and therefore is completely irrelevant to the replacement of a *log* file as claimed in the present application. Specifically, Schneier et al. describes:

> [A]n unalterable *log* should make it difficult for attackers to cover their tracks, meaning that the victims of the attack can quickly learn that their machine has been attacked, and take measures to contain the damage from that attack. The victims could then revoke some public key certificates, inform users that their data may have been compromised, *wipe the machine's storage devices and restore it from a clean backup*, or improve physical and network security on the machine to prevent further attacks.

(Section 5, paragraph 1, emphasis added.)

The above passage of Schneier et al. clearly describes that, based on a "log" file that records an attacker's attack on a machine, the owner of the machine (or the "victim") can "quickly learn" of the attack and take remedial measures, such as restoring "the machine's storage devices" "from a clean backup." This describes a conventional file backup/restore system, and does not at all teach or suggest restoring a *log file* itself (which records an attacker's attack) from a plurality of identical log files.

Note that in Schneier et al., several parallel log files are simply transmitted to their respective "trusted" computers for protection, and are *not* monitored for alteration or deletion. As such, in Schneier et al., any altered or deleted log file cannot be replaced with an unaltered log file from the several parallel log files. In other words, since Schneier et al. does not monitor its parallel log files for alteration or deletion, it cannot tell which log file has been altered or deleted, nor can it tell which log file remains unaltered and thus can be used to replace the altered/deleted log file.

In summary, Schneier et al. fails to teach or suggest the claimed features directed to "periodically monitoring the plurality of identical log files for alteration or deletion" and "replacing the altered or deleted log file with an unaltered log file from the plurality of identical log files." Consequently, Schneier et al. fails to teach each and every element of Claims 1 and 26,

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

and thus cannot anticipate Claims 1 and 26 under 35 U.S.C. § 102(a). Accordingly, Claims 1 and 26 are allowable over Schneier et al.

Claims 2-6, 8-21, and 23-25 all depend from Claim 1, and therefore are allowable for at least the same reasons why Claim 1 is allowable over Schneier et al.

Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS[PLLC]

Reg. no. 46,649
for

Shoko I. Leek
Registration No. 43,746
Direct Dial No. 206.695.1780

I hereby certify that this correspondence is being deposited with the U.S. Postal Service in a sealed envelope as first class mail with postage thereon fully prepaid and addressed to Mail Stop Appeal Brief—Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the below date.

Date: November 14, 2006

SIL:jam/vas

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS[PLLC]
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100